Synopsis of the Thesis

(Research Proposal)

"Analysis and design of novel framework for intrusion detection system using machine learning and deep learning"

SUBMITTED TO

School of Computational Sciences

SWAMI RAMANAND TEERTH MARATHWADA UNIVERSITY, NANDED (M. S.) INDIA

FOR THE AWARD OF THE DEGREE OF DOCTOR OF PHILOSOPHY

IN THE SUBJECT OF

COMPUTER SCIENCE

FACULTY OF SCIENCE AND TECHNOLOGY

By

ANIKET YADNESHWAR DIXIT

Under the Guidance of

Dr. S. B. THORAT
Director,
ITM College, Nanded

Research Center

School of computational sciences,
Swami Ramanand Teerth Marathwada University
Campus,Nanded Maharashtra, Year 2021-22

Table of Contents

Sr.No.	Title	Page No.
	Abstract	3
1.	Introduction	4
2.	Review of Literature	6
3.	Objectives of Research	7
4.	Methodology	7
5	Importance of study/ Society application	7
6.	Proposed Experiments	8
7.	References	11

Abstract

Intrusion detection is a defense system that can detect abnormal activity. Intrusion is defined as, "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource" [3], [32]. IDSs are forever measured as a subsequent wall of defense from the security point of analysis. IDSs can be deployed along with other security measures, such as access control, authentication mechanisms, and encryption techniques to better secure the systems against attacks. Using patterns of benign traffic or normal behavior or specific rules that describe a specific attack, IDSs can distinguish between normal and malicious actions [7], [32]. According to Dewa and Maglaras [8], [32], data mining, which is used to describe knowledge discovery can help to implement and deploy IDSs with higher accuracy and robust behavior compared to traditional IDSs that may not be as effective against modern sophisticated attacks [9], [32]. The necessity of IDSs is "low false-positive rate and high true positive rate". Intruders to a network can be classified into two types: external intruder and internal intruder.

(1) External intruder: An outsider using diverse means of attacks to arrive at the network.

(2) Internal intruder: The intrusion can be of any type such as attempted break, Masquerade, Penetration, Leakage, DoS and Malicious use. IDSs may provide partial detection solutions to those attacks. The perfect IDS would be able to detect all the intrusions listed above [4], [5], [6], [32]. Abuse detection: Here, the patterns must be defined and given to the system and act or behavior of nodes is compared with well-known attack patterns. Anomaly detection: The approach prime describes the real features of a "normal behavior", which are renowned using automated training and this method does not search for exact attack patterns, but in its place, it checks whether the behavior of the nodes can be measured as normal or anomalous. Research methodology facilitates smooth running of various operations, thereby making research as efficient possible, yielding the maximum information with minimum expenditure of effort, time and money. The research design stands for advanced planning of the methods to be adopted for collecting relevant information, tools and techniques to be used in the analysis of the objectives of the research. . In this work, the method used to construct Firstly we will used intrusion benchmark dataset to test the performance of machine learning based intrusion detection approaches. After that we will divide the benchmark dataset of intrusion in the two section that is Train Dataset and test dataset. It generate a model for detection of attack, With the help of test parameters like we will use performance indicators including accuracy, Precision, Recall, F1 Score. We will use the Google Colaboratory under python 3 using TensorFlow and Graphics Processing Unit (GPU) to perform experimentation. We will use NSL-KDD to test the performance of Machine learning based and deep learning based Algorithms for Intrusion detection approaches.

Keyword : NSL-KDD database, GPU-Graphics Processing Unit, IDS-Intrusion detection system.

1. Introduction

In today's world of network communications, network infiltration or network intrusion is the most pressing worry as well as main challenge .System attacks are becoming more common, which is a huge problem for system administrators. Various research projects are currently underway in order to find a successful and effective solution for preventing system infiltration and ensuring system security and protection. Intrusion in a network occur actively or passively, In a security system, if the initial systems of defense, "Intrusion Prevention," do not avoid intrusions, after that the succeeding system of protection, "Intrusion Detection," act. Intrusion Detection Systems (IDSs) present some or all of the following information to other supporting systems when they discover some suspicious behaviuor in a system. In any security issue, Intrusion Detection Systems (IDSs) present some or all of the following information to other supporting systems: detection of the intruder, the intruder's location (e.g., solitary node or district), the intrusion instance (e.g., date), intrusion activity (e.g., active or passive), intrusion type (e.g., wormhole, black hole, sinkhole, selective forwarding), and the layer where the intrusion occurs (e.g., wormhole, black hole, sinkhole, selective forwarding).

WSNs also have specific security objects

(1) Forward secrecy: preventing a node from decrypting any upcoming secret messages after it leaves the network. (2) Backward secrecy: preventing a joining node from decrypting any previously transmitted secret message. (3) Survivability: on the condition that a certain level of service in the attendance of failures. (4) Freshness: ensuring that the data are new and no adversary can repeat old messages. (5) Scalability: sustaining a large number of nodes. (6) Efficiency: measured storage, processing, and communication boundaries on sensor nodes [1], [32].

The researchers proposed several Intrusion Detection Systems (IDSs) to protect network from an adversary's intrusion. These IDS defence solutions are divided into two types: signature-based and anomaly-based. The former relies on signatures of known attack patterns, whereas the latter profiles a statistical usage model over time to classify data packets as normal or anomalous using techniques such as data mining, machine learning, deep learning and statistical modelling.

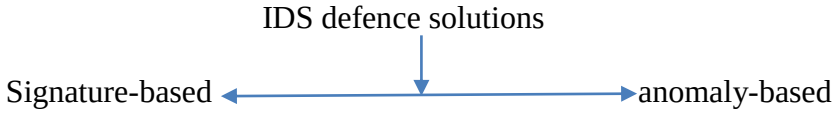

Figure 1 : Two main types of IDS by attack based

1.2 Intrusion Detection System (IDS)

In a network or system, any illegitimate or unapproved behaviour will be considered an "intrusion" An Intrusion Detection System (IDS) is a collection of tools, methods, and resources designed to aid in the detection, evaluation, differentiation, and description of intrusions. [2]. Intrusion detection is a type of defence system that detects unusual activity. "Any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource" [3]is defined as intrusion. IDSs are forever measured as a subsequent line of defence from a security standpoint. To better protect systems from attacks, IDSs can be used in conjunction with other security measures such as access control, authentication mechanisms, and encryption techniques. Using benign traffic patterns, normal behaviour, or specific rules that describe a specific types of attacks. Data mining, which is used to describe knowledge, according to Dewa and Maglaras When compared to traditional IDSs, which may not be as effective against modern sophisticated attacks [9], [32], discovery can assist in the implementation and deployment of IDSs with higher accuracy and robust behaviour. IDSs are required because they have a "low false-positive rate and a high true positive rate." External intruders and internal intruders are the two types of network intruders.

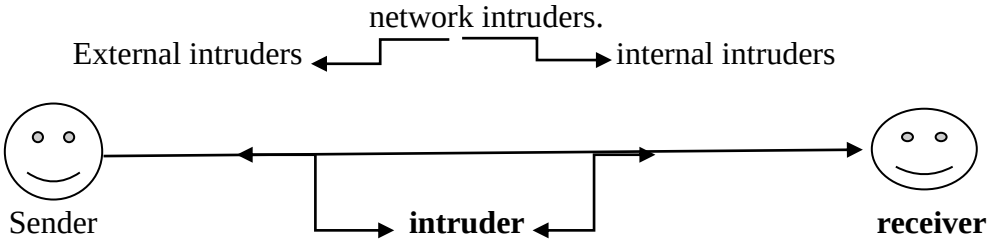

Figure 2 : Intrusion working and type.

(1) External intruder: An outsider who gains access to the network through a variety of means.
(2) Internal intruder: A compromised node that used to be a network associate. External and internal intruders can be detected by IDS, but internal intruders are more difficult to detect. This is because internal intruders have the necessary keying resources to by-pass any authentication mechanisms' protection. Any type of intrusion can occur, including attempted break, masquerade, penetration, leakage, DoS, and malicious use. IDSs may provide only a partial detection solution for such attacks. The ideal intrusion detection system would be capable of detecting all of the above-mentioned intrusions.[4],[5] IDS are classified into two types based on their deployment: host-based intrusion detection system (HIDS) and network-based intrusion detection system (NIDS) .HIDS is one of the measures on the host that are capable of detecting intrusions such as changes to important system files on the host, numerous failed access attempts to the host, abnormal method memory allocations, unusual CPU activity, or I/O activity. HIDS accomplishes this by monitoring the host's real-time scheme usage or by investigating log files on the host. NIDS can examine a whole packet, its payload, IP addresses, or ports passively or actively by listening to network transmissions. IDS can be classified based on detection methodologies.
IDS can be divided into three types: abnormality-based detection, abuse-based detection, and specific-based discovery.

1} Abuse detection: In this case, the patterns must be defined and given to the system, and node actions or behaviours are compared to well-known attack patterns. The disadvantages of this method are that it requires knowledge to build attack patterns and it cannot detect novel attacks. The disadvantage of this approach is that it significantly reduces system management efficiency because the network administrator must always provide IDS agents with a current database.

2) Anomaly detection: The approach prime describes the true features of "normal behaviour," which are recognized using automated training, and this method does not search for exact attack patterns, but rather checks whether the behaviour of the nodes can be measured as normal or anomalous. Then, any behaviour that deviates from these behaviours is flagged as an intrusion. If a sensor node does not act according to the distinct specification of a particular protocol, the IDS would have high confidence in determining that the node is malicious; incorrect decisions made by IDS in terms of false-positive and false-negative alarms influence detection accuracy. The disadvantage of this method is that the system can show valid but hidden behavior the path to a high false alarm rate. 3) Detection based on specifications: As this method combines the goals of misuse and anomaly detection mechanisms, it focuses on discovering deviations from normal behaviour that are not defined by machine learning techniques or training data. The specifications that describe what is considered normal behaviour are defined manually, and action is taken in accordance with these specifications. The disadvantage of this approach is that all specifications must be developed manually, which is a time-consuming procedure for humans, and it cannot detect malicious behaviours that do not violate the IDS protocol's defined specifications. Misuse and anomaly-based detection techniques can sometimes be used, giving rise to hybrid detection mechanisms.[1]

Review of Literature (Literature Survey)

Myint and Meesad suggested an incremental learning technique based on SVM as a classifier [11]. This approach uses SVM for Prediction to reduce the number of steps necessary for calculation, the algorithm's complexity, the error set, and the time spent continually training the dataset. The author evaluated the system's performance using the KDD Cup99 dataset in this method. The proposed system is capable of predicting 41 characteristics of the incoming dataset.

M. Nabila Farnaaz and Nabila Farnaaz

A. Jabbar suggested an intrusion detection approach based on a Random Forest classifier [12].

The author used RF as an ensemble classifier in this technique, and the model outperforms other standard classifiers when it comes to categorization of attacks

The author employed the NSL KDD dataset to evaluate the model's performance, and the propose d model is effective, with a low false alarm rate and a high detection rate.

Majjed et al. introduced the STL-IDS aided self-taught learning framework as an effective deep learning approach [13].

The proposed approach can be utilised for feature learning and dimension reduction.

To improve SVM prediction accuracy, this strategy reduces the training and testing time.

is lowered The proposed approach improves the detection of network intrusions

The decision tree for intrusion detection was assessed by Sandhya Peddabachigari et al. [14]. The 1998 DARPA dataset was used to evaluate intrusion detection using the decision, and the system outperformed standard models in terms of accuracy. In comparison to the support vector machine, the results reveal that the training and testing times are shorter.

In WSN [16], Wenchao Li et al. proposed a new intrusion detection system based on the K-nearest classification algorithm. The proposed system is used to distinguish between normal and abnormal nodes by observing unusual behaviour. The parameter selection and error rate of the intrusion detection system are examined in this approach. The proposed model performs better in terms of efficiency, with a high detection rate and speed.

Michael Riecker et al. [19] propose a lightweight, energy-efficient system that detects intrusions using mobile agents and the energy utilisation of sensor nodes as a metric. To forecast energy consumption, a linear regression model is used. The authors assess the proposed detection algorithm in terms of detection accuracy in a scenario involving flooding and a black hole attack. They also investigate the effect of history size and walking strategies on detection time. They do not require nodes to monitor their environment or collaborate, nor do they require audit data to be transferred to a central point. Instead, use a mobile agent that collects energy readings and sends an alert if there are any sudden changes. The viability of mobile intrusion detection agents

It has been demonstrated in wireless sensor networks. The authors also demonstrated that energy consumption is an appropriate metric for detecting denial-of-service attacks. They tested their proposed intrusion detection method in simulations and achieved high detection accuracy while maintaining a low false-positive rate.

Mohammad Wazid et al. [20] proposed a secure intrusion detection approach that uses K-means clustering to extend the lifespan of WSNs. The authors proposed a new intrusion detection technique for a hybrid anomaly; K-means automatically built attack patterns over training data for detection.

The authors evaluate the approach using a WSN dataset generated with the Opnet modeller and co ntaining a variety of attributes such as end-to-end delay, traffic sent and traffic received. The training dataset contains the network parameters' d efault values.

The testing dataset is generated in an actual working model and consists of normal and abnormal n etwork parameter values.

The authors claim that the proposed scheme achieves a detection rate of 98.6 percent and a false-positive rate of 1.2 percent, which is better than existing related schemes, and that the proposed te chnique can detect two types of malicious nodes: black hole and misdirection nodes.

Aim and objectives

1. Aim:
    1. Provide a detailed comprehensive evaluation and comparison of existing frameworks to detect intrusion in the network.
    2. Design and implement a new framework to detect intrusion.

2. Objectives:

    a. To study the existing frameworks to detect intrusion in network.
    b. To study the advantages and disadvantages of existing frameworks.
    c. To study the intrusion dataset like NSL-KDD.

    d. Designing a novel framework based on the machine learning, Deep learning technique to detect intrusion in network.

2. Research Methodology:

Research methodology facilitates smooth running of various operations, thereby making research as efficient possible, yielding the maximum information with minimum expenditure of effort, time and money. The research design stands for advanced planning of the methods to be adopted for collecting relevant information, tools and techniques to be used in the analysis of the objectives of the research. In this work, the method used to construct research consists of following five parts:

Part 1: Study of Networks, network attacks.

Part 2: Study of Machine Learning Techniques.

Part 3: Study of the application of machine learning techniques in the field of network security.

Part 4: Building and applying machine learning models to detect intrusion in network.

Part 5: Designing a new framework for network security.

3. Importance of study/ Society application

1. To detect intrusion in network.

2. To secure network.

Proposed Experiments

In the research work proposed experimental approach we will be use in a way of flow shown in the figure 3 : flow chart of proposed framework.

Firstly we will used intrusion benchmark dataset to test the performance of machine learning based intrusion detection approaches. After that we will divide the benchmark dataset of intrusion in the two section that is Train Dataset and test dataset.

In the train dataset section in this we will use a section of benchmark dataset of 70% of data in it, so has to train 70% of data with machine learning algorithm with this 30% of remain dataset in test dataset.

It generate a model for detection of attack weather the model is used for appropriate and best fit in the form of detection of attack working.

It will generate and alert for it and after that we will use evaluation parameter for testing how much 'efficiency' of this model goes to generate.

With the help of test parameters like we will use performance indicators including accuracy, Precision, Recall, F1 Score.

We will use the Google Colaboratory under python 3 using TensorFlow and Graphics Processing Unit (GPU) to perform experimentation. We will use NSL-KDD to test the performance of Machine learning and deep learning based Intrusion detection approaches.(fig.3) We will use the most important performance indicators, including accuracy, Precision, Recall, F1 Score.

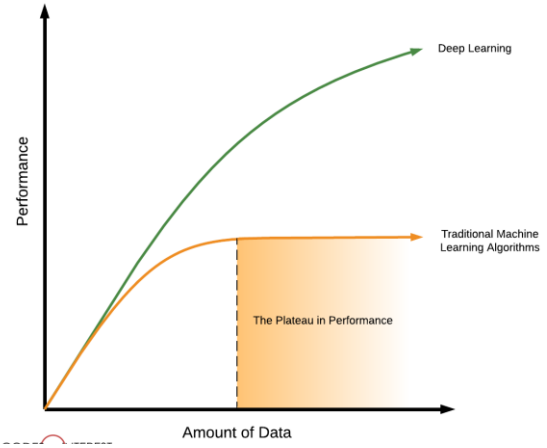

Figure 3 : Deep learning and Machine Learning approach

1For this function, we used the NSL-KDD database as input. The NSL-KDD database consists of two parts, namely, the train database and the test database. The database has 41 elements, and 1 element is considered a prediction label.

LIST OF NSL-KDD DATASET FILES AND THEIR DESCRIPTION
1KDDTrain+.ARFF
The full NSL-KDD train set with binary labels in ARFF format
2 KDDTrain+.TXT
The full NSL-KDD train set including attack-type labels and difficulty level in CSV format
3 KDDTrain+_20Perce nt.ARFF
A 20% subset of the KDDTrain+.arff file
4 KDDTrain+_20Perce nt.TXT
A 20% subset of the KDDTrain+.txt file
5 KDDTest+.ARFF
The full NSL-KDD test set with binary labels in ARFF format
6 KDDTest+.TXT
The full NSL-KDD test set including attack-type labels and difficulty level in CSV format
7 KDDTest-21.ARFF
A subset of the KDDTest+.arff file which does not include records with difficulty level of 21 out of 21

8 KDDTest-21.TXT
A subset of the KDDTest+.txt file which does not include records with difficulty level of 21 out of 21
The analysis on the NSL-KDD dataset show that it is a best candidate data set to simulate and test the performance of IDS in general way with -Duration, Protocol_type, service, flag, Src_bytes, Dst_bytes, Land, Wrong_fragment, Urgent, Hot, Num_failed _logins, Logged_in, Num_comp romised, Root_shell, Su_attempted, Num_root, Num_file_c reations, Num_shells, Num_acces s_files, Num_outbound_cmds, Is_hot_login, Is_guest_login,count, Srv_count, Serror_rate, Srv_serror_rate, Rerror_rate, Srv_rerror_rate, Same_srv_rate, Diff_srv_rate, Srv_diff_host_ rate, Dst_host_count, Dst_host_srv_ count, Dst_host_same _srv_rate, Dst_host_diff_ srv_rate, Dst_host_same _src_port_rate, Dst_host_srv_ diff_host_rate, Dst_host_serro r_rate, Dst_host_srv_serror_rate, Dst_host_rerro r_rate, Dst_host_srv_rerror_rate, all these are the features with 41in number.

- TensorFlow

TensorFlow is a software library or framework, designed for the Google team to use ML and deep learning ideas easily. It incorporates a computational algebra of simple calculation techniques for simple mathematical expressions. TensorFlow is an AI library that helps developers build large, multi-layer neural networks using data flow graphs. TensorFlow also facilitates the development of Deep Learning models, compresses ML / AI technology and allows easy submission of ML-enabled applications. TensorFlow works best when it comes to categories, understanding, finding, predicting and building data.
TensorFlow Features:

- It incorporates an element of what it describes, amplifies and calculates mathematical expressions easily with the help of a multi-sided system called tensors.

Includes support for the planning of deep neural networks and machine learning strategies

Test parameters
We used the most important performance indicators, including, precision, recall, F1 score and accuracy. We can calculate performance metrics us2ing the following
Accuracy: It is a metaphor used to indicate the proportion of appropriate categories of records in total in a test set. Accuracy shows the division into categories N all examples were correct.
Accuracy = (TP + TN) / (TP + FN + TN + FP)
Precision (P): It is a metaphor that measures actual performance within the required response space, i.e., between positions. Precision indicates the value of the system to get network threat that actual entry was found. The higher the P value, the lower the false alarm rate.
P = TP / (TP + FP)
Recall (R): It is a metaphor for how many predicted responses are discarded or for each appropriate label, and how many other true labels we discard. Recall shows a number of positive examples that are well divided. We want a higher value of R.
R = TP / (TP + FN)
F1 (F) Score: It is a harmonic definition of two matrics P and R By transferring the balance between accuracy and recall, it provides a better measure of accuracy. We want a maximum value of F.
$F = (2 * P * R) / (P + R)$
Where,
True positive (TP): It can be outlined as anomaly instances properly categorized as an anomaly.
False positive (FP): It can be outlined as normal situations wrongly categorized as an anomaly.
True negative (TN): It can be outlined as normal situations properly categorized as normal.
False negative (FN): It can be outlined as anomaly instances wrongly categorized as normal.
Python
Python is a translation that is translated into general, interactive, object-oriented, and advanced. It was built by Guido van Rossum between 1985-1990. Python is a popular platform used for R&D production programs. It is a great language with several modules, packages and libraries that provide many ways to accomplish the task.

Python and its libraries such as NumPy, SciPy, Sikit, Matplotlib are used for scientific testing and data analysis. They are also widely used to create unparalleled ML algorithms.
Python provides a framework designed to perform data mining operations on large amounts of data successfully in a short amount of time. It includes a number of applications achieved with algorithms such as Naïve Bayes, KNN and Random Forest.

Python Features

- Supports procedural, frameworked and object oriented programming.
- It can be used as a scripting language to create large programs.
- It provides the most powerful data types and supports dynamic type viewing.
- Supports automatic garbage collection.
- It can be easily integrated with C, C ++, COM, ActiveX, CORBA, and Java.

Benefits of Python

- Easy-to-learn - Python has a few keywords, simple layout, and simple syntax.
- Easy-to-maintain - Python source code is easy to maintain.
- Standard General Library
- Interaction mode - Python supports interaction mode that allows interaction testing and correction of captions errors.
- Portable - Python can work on a variety of computer platforms and has the same interface across all platforms.
- Extensible - You can add low-level modules to a Python interpreter. These modules enable programmers to add or customize their tools to work better.
- Database - Python provides integration into all major commercial data.
- GUI Programming - Python supports GUI applications that can be created and sent to multiple system calls, libraries and windows programs, such as Windows MFC, Macintosh, and the Unix program.
- Scalable - Python provides better framework and support for larger programs than the Shell script

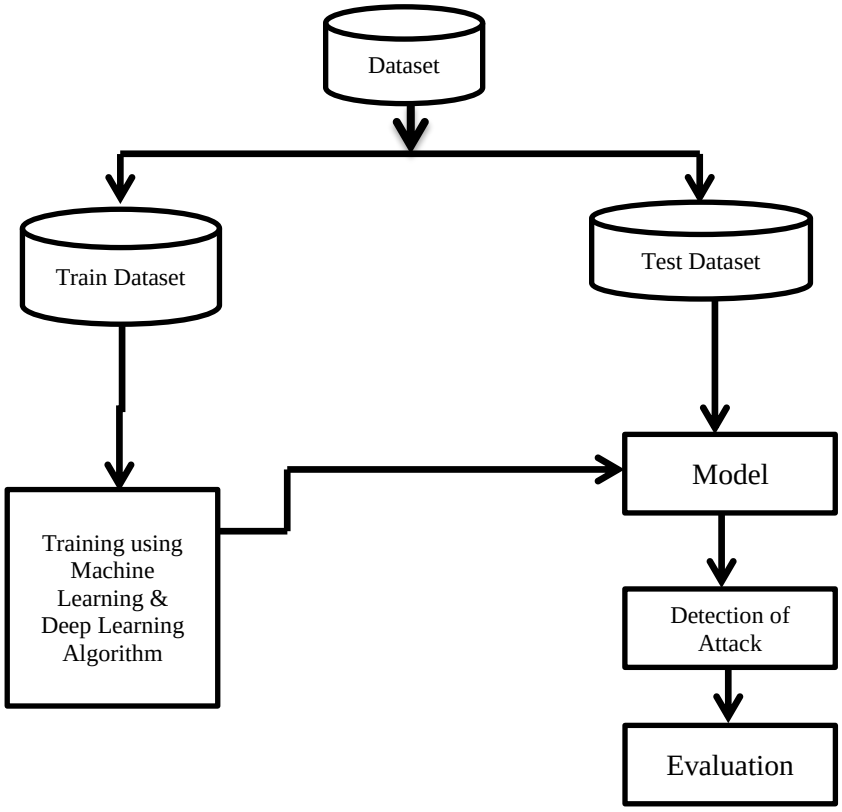

Figure 3 : FLOWCHART OF PROPOSED FRAMEWORK

5. References:

[1]I.SumaiyaThaseen1,J.SairaBanu2,K.Lavanya2,Muhammad Ghalib2, KumarAbhishek3, "An integrated intrusion detection system using correlation-based attribute selection and artificial neural network", John Wiley &Sons ,Ltd, 2020.

[2] Samrat Kumar Dey, Md. Raihan Uddin and Md. Mahbubur Rahman, "Chapter 41 ,Performance Analysis of SDN-Based Intrusion Detection Model with Feature Selection Approach" Springer Nature Singapore Pte Ltd. 2020.

[3] Pankaj R. Chandre, Parikshit N. Mahalle and Gitanjali R. Shinde, "Deep Learning and Machine Learning Techniques for Intrusion Detection and Prevention in Wireless Sensor Networks: Comparative Study and Performance Analysis" Springer Nature Singapore Pte Ltd. 2020.

[4] T. Tulasi Bhavani, M. Kameswara Rao and A. Manohar Reddy, "Network Intrusion Detection System Using Random Forest and Decision Tree Machine Learning Techniques" ,Springer Nature Singapore Pte Ltd. 2020.

[5] Nicholas Lee, Shih Yin Ooi and Ying Han Pang, "A Sequential Approach to Network Intrusion Detection" Springer Nature Singapore Pte Ltd. 2020.

[6] Mukaram Safaldin1 ,Mohammed Otair1 ,Laith Abualigah1, "Improved binary gray wolf optimizer and SVM for intrusion detection system in wireless sensor networks", springer2020.

[7] Mohamed Amine Ferrag, Leandros Maglaras, Sotiris Moschoyiannis, Helge Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study", Journal of Information Security and Applications, 50 (2020) 102419.

[8] Dewa Z, Maglaras L A, "Data mining and intrusion detection systems", Int. J. Adv. Comput. Sci. Appl. 2016; 7(1):62–71.

[9] Stewart B , Rosa L , Maglaras LA , Cruz TJ , Ferrag MA , Simões P , et al., "A novel intrusion detection mechanism for scada systems which automatically adapts to network topology changes", EAI Endorsed Trans. Ind. Netw. Intell. Syst. 2017; 4(10):e4.

[10]Niyaz, Q., Sun, W., Javaid, A. Y., & Alam, M. (2015, December 03–05), "A deep learning approach for network intrusion detection system", In BICT 2015, New York City, United States.

[11]Myint, H. O., & Meesad, P. (2009), "Incremental Learning Algorithm based on Support Vector
Machine with Mahalanobis distance (ISVMM) for Intrusion Prevention", 978-1-4244-3388 9/09/$25.00 ©2009 IEEE.

[12]Farnaaz, N., & Jabbar, M. A. (2016). Random forest modelling for network intrusion detection system. Procedia Computer Science, 89, 213–217 (Elsevier).

[13] Al-Qatf, M., Lasheng, Y., Alhabib, M., & Al-Sabahi, K. (2018), "Deep learning approach combining sparse auto encoder with SVM for network intrusion detection", IEEE Access. https:// doi.org/10.1109/ACCESS.2018.2869577.

[14] Peddabachigari, S., Abraham, A., & Thomas, J. (2016), "Intrusion detection systems using decision trees and support vector machines", International Journal of Advanced Networking and Applications, 07(04), 2828–2834. ISSN: 0975-0290.

[15] Panda, M., & Patra, M. R. (2007, December). "Network intrusion detection using Naïve Bayes", IJCSNS International Journal of Computer Science and Network Security, 7(12).

[16] Li, W., Yi, P., Wu, Y., Pan, L., & Li, J. (2014), "A new intrusion detection system based on KNN classification algorithm in WSN", Journal of Electrical and Computer Engineering, 2014 (Hindawi Publishing Corporation).

[17] Van, N. T., Thinh, T. N., & Sach, L. T. (2017), "An anomaly-based network intrusion detection system using deep learning", In 2017 International Conference on System Science and Engineering (ICSSE).

[18]Yang, Y., Zheng, K., Wu, C., Niu, X., Yang, Y., "Building an Effective Intrusion Detection System Using the Modified Density Peak Clustering Algorithm and Deep Belief Networks", Appl. Sci. 9, 238 (2019).

[19] Michael Riecker, Sebastian Biedermann, Rachid El Bansarkhani and Matthias Hollick, "Lightweight energy consumption-based intrusion detection system for wireless sensor networks", International Journal of Information Security, vol. 14, no. 2, pp. 155-167, 2015.

[20] Mohammad Wazid and Ashok Kumar Das, "An Efficient Hybrid Anomaly Detection Scheme

Using K- Means Clustering for Wireless Sensor Networks", Wireless Personal Communications, vol. 90, no. 4, pp. 1971-2000, October 2016.
[21]Ahmed Saeed, Ali Ahmadinia, Abbas Javed and Hadi Larijani, "Random Neural Network based Intelligent Intrusion Detection for Wireless Sensor Networks", In proceedings of International Conference on Computational Science, vol. 80, pp. 2372-2376, 2016.
[22]Yassine Maleh, Abdellah Ezzati, Youssef Qasmaoui and Mohamed Mbida, "A Global Hybrid Intrusion Detection System for Wireless Sensor Networks", The fifth International Symposium on Frontiers in Ambient and Mobile Systems, vol. 52, pp. 1047-1052, 2015.
[23]Hichem Sedjelmaci and Mohamed Feham, "Novel Hybrid Intrusion Detection System for Clustered Wireless Sensor Network", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.4 July 2011.
[24]P. R. Chandre, P. N. Mahalle, and G. R. Shinde, "Deep Learning and Machine Learning Techniques for Intrusion Detection and Prevention in Wireless Sensor Networks: Comparative Study and Performance Analysis", Lecture Notes in Networks and Systems 82, https://doi.org/10.1007/978-981-13-9574-1_5
[25]Nicholas Lee, Shih Yin Ooi and Ying Han Pang, " A Sequential Approach to Network Intrusion Detection", Lecture Notes in Electrical Engineering 603, https://doi.org/10.1007/978-981-15-0058-9_2
[26]Kishor Kumar Gulla, P. Viswanath, Suresh Babu Veluru, and R. Raja Kumar, " Machine Learning Based Intrusion Detection Techniques", Handbook of Computer Networks and Cyber Security, https://doi.org/10.1007/978-3-030-22277-2_35
[27]Tavallaee M, Bagheri E, Lu W, Ghorbani A. A. "A detailed analysis of the kdd cup 99 data set", In: 2009 IEEE Symposium on Computational Intelligence for Security and Defence Applications. IEEE; 2009. p. 1–6.
[28]Nsl kdd. https://www.unb.ca/cic/datasets/nsl.html
[29]L. Dhanabal, and Dr. S.P. Shantharajah, "A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms", international Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 6, June 2015.
[30]Sapna S. Kaushik, Dr. Prof. P. R. Deshmukh, "Detection of Attacks in an Intrusion Detection System", International Journal of Computer Science and Information Techytre4wsnologies, Vol. 2 (3), 2011, 982-986.
[31] Opeyemi Osanaiye, Olayinka Ogundile, Folayo Aina, Ayodele Periola, "FEATURE SELECTION FOR INTRUSION DETECTION SYSTEM IN A CLUSTER-BASED HETEROGENEOUS WIRELESS SENSOR NETWORK", FACTA UNIVERSITATIS, Series: Electronics and Energetics Vol. 32, N o 2, June 2019, pp. 315-330, https://doi.org/10.2298/FUEE1902315O.
[32] Seema M.Shinde, Dr.Thorat S.B. , Miss.Tazeen Khan, Dr.PravinTamsekar,"Survey and performance analysis of Machine learning based Intrusion detection approaches in wireless sensor networks", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 22, Issue 4, Ser. II (Jul. – Aug. 2020), PP 06-13.
[33] Carolin Strobl, Anne-Laure Boulesteix, Achim Zeileis and Torsten Hothorn, "Bias in random forest variable importance measures: Illustrations, sources and a solution", BMC Bioinformatics 2007, 8:25 doi:10.1186/1471-2105-8-25
[34] Rakesh Sharma, and Vijay Anant Athavale, "A Survey of Intrusion Detection Techniques and Architectures in Wireless Sensor Networks", Int. J. Advanced Networking and Applications, Volume: 10 Issue: 04 Pages: 3925-3937, 2019.
[35] M. Ngadi, A.H. Abdullah, and S. Mandala, "A survey on MANET intrusion detection", International J. Computer Science and Security, volume 2, number 1, pages 1-11, 2008.
[36] Y. Zhang, W. Lee, and Y.A. Huang, "Intrusion detection techniques for mobile wireless networks", J. Wireless Networks, vol. 9, num. 5, pp.545-556, 2003.
[37] T.S. Sobh, "Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art", Elsevier J. Computer Standards and Interfaces, volume 28, number 6, pages 670-694, 2006.
[38] T. Anantvalee and J. Wu, "A survey on intrusion detection in mobile ad hoc networks",

Springer J. Wireless Network Security, pages 159-180, 2007.
[39] P. Albers, O. Camp, J. Percher, B. Jouga, L. M, and R. Puttini, "Security in Ad Hoc Networks: A General Intrusion Detection Architecture Enhancing Trust Based Approaches," Proc. 1st International Workshop on Wireless Information Systems (WIS-2002), pp. 1-12, April 2002.
[40] Mohamed Amine Ferrag, Leandros Maglaras, Sotiris, Helge Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study" Elsevier 2019.

Date:
Place:

Research Guide
Dr. S.B. Thorat
Director
ITM College, Nanded

Research Student
Mr. Aniket Yadneshwar Dixit